

actual names is from the ISPs to which Defendants subscribe and from which Defendants obtain Internet access. This information is readily available to the ISPs from documents they keep in the regular course of business.¹

For the past few years, federal district courts throughout the country, including this Court, have granted expedited discovery in Doe Defendant lawsuits that are factually similar, if not identical, to the instant lawsuit.² In these cited cases and others like them, copyright holder plaintiffs have obtained the identities of P2P network users from ISPs through expedited discovery using information similar to that gathered by Plaintiff in the instant case, and they have used that information as the basis for their proposed subpoenas to these ISPs. Plaintiff respectfully requests that this Court follow the well-established precedent, and grant this motion for expedited discovery against those ISPs listed in Exhibit A (*see* Compl., Ex. A), together with various other ISPs operating both within and outside the District of Columbia that Plaintiff later discovers, during the course of this litigation, were the actual entities providing the Doe Defendants with online services and/or network access, and all of their respective subsidiaries,

¹ Because Plaintiff does not currently know the identity of any of the Defendants, Plaintiff cannot ascertain the position of any of the Defendants on this Motion.

² Such cases include, but are not limited to: *Metro-Goldwyn-Mayer Pictures Inc. v. Does 1–10*, No. 04-2005 (JR) (D.D.C.) (Robertson, J.); *Twentieth Century Fox Film Corp., et al. v. Does 1–9*, No. 04-2006 (EGS) (D.D.C.) (Sullivan, J.); *Lions Gate Films, Inc., et al. v. Does 1–5*, No. 05-386 (EGS) (D.D.C.) (Sullivan, J.); *UMG Recordings, et al. v. Does 1–199*, No. 04-093 (CKK) (D.D.C.) (Kollar-Kotelly, J.); *Caroline Records, Inc. v. Does 1–175*, No. 04-2028 (D.D.C.) (Lamberth, J.); *Paramount Pictures Corp. v. Does 1–8*, No. 05-535 (D.N.J.) (Wolfson, J.); *Columbia Pictures Indus., Inc. v. Doe*, No. CV05-0134Z (W.D. Wash.) (Zilly, J.); *Warner Bros. Entm't Inc. v. Does 1–7*, No. 05 CV 0883 (S.D.N.Y.) (Cote, J.); *Screen Gems, Inc. v. Does 1–34*, No. SA04CA1038OG (W.D. Tex.) (Garcia, J.); *Columbia Pictures Indus., Inc. v. Does 1–10*, No. 1:05CV515-BBM (N.D. Ga.) (Martin, J.); *Lions Gate Films, Inc. v. Does 1–23*, No. 04 C 7398 (N.D. Ill.) (Gottschall, J.); *Paramount Pictures Corp. v. Does 1–11*, No. 4 05CV00335CAS (E.D. Mo.) (Shaw, J.); *Columbia Pictures Indus., Inc. v. Doe (67.123.19.140)*, No. C 04 5243 PJH (N.D. Cal.) (Hamilton, J.); *Metro-Goldwyn-Mayer Pictures Inc. v. Does 1–2*, No. 05CV0761-B(POR) (S.D. Cal.) (Porter, J.); *Disney Enter., Inc. v. Does 1–18*, No. 05-RB-339(CBS) (D. Colo.) (Shaffer, J.).

parent companies and affiliates who may possess identifying data for the Doe Defendants (collectively, the “ISPs”).

As alleged in the complaint, the Doe Defendants, without authorization, converted Plaintiff’s Work into a video file using a “DVD ripper”. Defendants then used an online peer-to-peer (“P2P”) media distribution system to upload/download the copyrighted Work and distribute it to other users on the P2P network, including by making the copyrighted Work for which Plaintiff holds the exclusive sale and distribution rights available for distribution to others. In the instant case, the manner of the transfer of files amongst the P2P network users is called a “BitTorrent protocol” or “torrent” which is different than the standard P2P protocol used for such networks. (*See* Compl.; Hansmeier Decl. ¶ 6, attached to this Motion as Exhibit A.) The BitTorrent protocol makes even small computers with low bandwidth capable of participating in large data transfers across a P2P network. It has been estimated that it accounts for approximately 27–55% of all Internet traffic (depending on geographical location) as of February 2009.³ The initial file-provider intentionally elects to share a file with a torrent network. This initial file is called a seed. Other users (“peers”) on the network connect to the seed file to download. As yet additional peers request the same file each additional user becomes a part of the network from where the file can be downloaded. However, unlike a traditional P2P network, each new file downloader is receiving a different piece of the data from each user who has already downloaded the file that together comprise the whole (this piecemeal system with multiple pieces of data coming from peer members is called a “swarm”). Thus, every downloader is also an uploader. This means that every “node” or peer user who has a copy of the infringing copyrighted material on a torrent network must necessarily also be a source of download for that

³ *BitTorrent Still King of P2P Traffic*, TorrentFreak (Feb. 18, 2009), <http://torrentfreak.com/bittorrent-still-king-of-p2p-traffic-090218>.

infringing file. This distributed nature of BitTorrent leads to a rapid viral spreading of a file throughout peer users. As more peers join the swarm, the likelihood of a successful download increases. Because of the nature of a BitTorrent protocol, any seed peer who has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a source for the subsequent peer so long as that first seed peer is online at the time the subsequent peer downloads a file. Essentially, because of the nature of the swarm downloads as described above, every infringer is *simultaneously* stealing copyrighted material from many ISPs in numerous jurisdictions around the country. (*See* Hansmeier Decl. ¶¶ 6–7.)

Because Defendants used fictitious network names or pseudonyms when they swarmed and distributed Plaintiff’s copyrighted Work, Plaintiff does not know the Defendants’ actual identities. (*See* Hansmeier Decl. ¶ 15.) However, Plaintiff has identified each Defendant by a unique Internet Protocol (“IP”) address assigned to that Defendant by his/her ISP on the date and at the time of the Defendant’s infringing activity. (*See id.* ¶ 16.) Plaintiff also made a copy of substantial portions of the Work that each Defendant unlawfully distributed or made available for distribution through the file sharing networks, and confirmed that such file contained the Work that was copyrighted by Plaintiff. (*See id.* ¶ 19.) All of this information was gathered by an on-line piracy technology specialist at 6881 Forensics, LLC (“6881”). 6881 used specific technology, software, systems, and procedures that were designed to ensure that the information gathered about each Doe Defendant is accurate. (*See generally id.*)

Plaintiff has identified certain ISPs that provided Internet access to each Defendant, and assigned the unique IP address to the Defendant, from information provided to it by 6881, which used its proprietary tracing software program to trace the IP address for each Defendant. (*See* Hansmeier Decl. ¶¶ 15–16.) When given a Defendant’s IP address and the date and time of the

infringing activity, an ISP can identify the name and address of the Doe Defendant (i.e., the ISP's subscriber), as well as the date of the infringing activity, because that information is contained in the ISP's subscriber activity log files. (*See id.* ¶¶ 21–22.) Infringement of Plaintiff's Work is on-going and continuous by other parties in addition to the Doe Defendants currently identified by Plaintiff. Accordingly, Plaintiff continues to monitor torrent-based infringement of its Work (*see id.* ¶ 24), and seeks the ability to pursue claims for copyright infringement against later-identified infringers.

ISPs typically keep log files of subscriber activities for only limited periods of time—sometimes for as little as weeks or even days—before erasing the data. (*See* Hansmeier Decl. ¶ 22.) However, some ISPs lease or otherwise allocate certain of their IP addresses to other unrelated, intermediary ISPs. (*See id.* ¶ 23.) Since these lessor ISPs, as a consequence, have no direct relationship—customer, contractual, or otherwise—with the end-user, they are unable to identify the Doe Defendants through reference to their user logs. (*Id.*) The intermediary ISPs, though, should be able to identify the Doe Defendants by reference to their own user logs and records. Accordingly, Plaintiff seeks leave to serve on the ISPs it has identified, and continues to identify as it continues to monitor torrent-based infringement of Plaintiff's Work (*see id.* ¶ 24), limited, immediate discovery sufficient to determine the Doe Defendants' true identities. To the extent that any ISP, in turn, identifies a different entity as the ISP providing network access and online services to the Doe Defendants, Plaintiff also seeks leave to serve, on any such later identified ISP, limited discovery sufficient to identify the Doe Defendant prior to the Rule 26 conference.

Plaintiff requests permission to serve a Rule 45 subpoena on the ISPs it has identified as of this date, and those it identifies in the future, the true name, address, telephone number, e-mail

address, and Media Access Control (“MAC”) address (data available only to the ISPs that identifies the specific computer used for the infringing activity) of each Doe Defendant that it has identified to date, and those it identifies in the future during the course of this litigation. Plaintiff will only use this information to prosecute the claims made in its Complaint. Without this information, Plaintiff cannot pursue its lawsuit to protect its Work from ongoing and repeated infringement. (*See* Hansmeier Decl. ¶ 21.)

If the Court grants this Motion, Plaintiff will serve a subpoena on the ISPs requesting the identifying information within fifteen (15) business days. If the ISPs cannot itself identify one or more of the Doe Defendants but does identify an intermediary ISP as the entity providing online services and/or network access to such Defendants, Plaintiff will then serve a subpoena on that ISP requesting the identifying information for the relevant Doe Defendants within fifteen (15) business days. In either case, these ISPs will be able to notify their subscribers that this information is being sought, and each Defendant will have the opportunity to raise any objections before this Court prior to the return date of the subpoena. Thus, to the extent that any Defendant wishes to object, he or she will be able to do so.

II. ARGUMENT

Courts routinely allow discovery to identify “Doe” defendants. *See, e.g., Wakefield v. Thompson*, 177 F.3d 1160, 1163 (9th Cir. 1999) (holding that it was error to dismiss unnamed defendants given possibility that identity could be ascertained through discovery); *Valentin v. Dinkins*, 121 F.3d 72, 75–76 (2d Cir. 1997) (finding that plaintiff should have been permitted to conduct discovery to reveal identity of defendant); *Dean v. Barber*, 951 F.2d 1210, 1215 (11th Cir. 1992) (holding that it was error to deny plaintiff’s motion to join John Doe defendant where identity of John Doe could have been determined through discovery); *Munz v. Parr*, 758 F.2d

1254, 1257 (8th Cir. 1985) (“Rather than dismissing the claim, the court should have ordered disclosure of Officer Doe’s identity . . . or permitted the plaintiff to identify the officer through discovery.”); *Maclin v. Paulson*, 627 F.2d 83, 87 (7th Cir. 1980) (finding that where “party is ignorant of defendants’ true identity . . . plaintiff should have been permitted to obtain their identity through limited discovery”); *Gillespie v. Civiletti*, 629 F.2d 637, 642 (9th Cir. 1980) (“[W]here the identity of alleged defendants [are not] known prior to the filing of a complaint . . . the plaintiff should be given an opportunity through discovery to identify the unknown defendants”); *Murphy v. Goord*, 445 F. Supp. 2d 261, 266 (W.D.N.Y. 2006) (finding that in situations where the identity of alleged defendants may not be known prior to the filing of a complaint, the plaintiff should have an opportunity to pursue discovery to identify the unknown defendants); *Equidyne Corp. v. Does 1–21*, 279 F. Supp. 2d 481, 483 (D. Del. 2003) (allowing pre-Rule 26 conference discovery from ISPs to obtain identities of users anonymously posting messages on message boards). In similar copyright infringement cases brought by motion picture studios and record companies against Doe defendants, courts, including this Court, have consistently granted plaintiffs’ motions for leave to take expedited discovery to serve subpoenas on ISPs to obtain the identities of Doe Defendants prior to a Rule 26 conference. *See Warner Bros. Records, Inc. v. Does 1–6*, 527 F. Supp. 2d 1, 2 (D.D.C. 2007) (Sullivan, J.) (citing Mem. Op. & Order, *UMG Recordings, Inc. v. Does 1–199*, No. 04-093 (D.D.C. Mar. 10, 2004) (Kollar-Kotelly, J.); Order, *UMG Recordings v. Does 1–4*, 64 Fed. R. Serv. 3d 305 (N.D. Cal. Mar. 6, 2006)) (allowing plaintiffs to serve a Rule 45 subpoena upon Georgetown University to obtain the true identity of each Doe defendant, including each defendant’s true name, current and permanent addresses and telephone numbers, email address, and Media Access Control (“MAC”) address).

Courts consider the following factors when granting motions for expedited discovery to identify anonymous Internet users: (1) whether the plaintiff can identify the missing party with sufficient specificity such that the Court can determine that defendant is a real person or entity who could be sued in federal court; (2) all previous steps taken by the plaintiff to identify the Doe Defendant; and (3) whether the plaintiff's suit could withstand a motion to dismiss. *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578–80 (N.D. Cal. 1999); *see also Rocker Mgmt. LLC v. Does*, No. 03-MC-33, 2003 WL 22149380, at *1–2 (N.D. Cal. May 28, 2003) (applying *Seescandy.com* standard to identify persons who posted libelous statements on Yahoo! Message board; denying request for expedited discovery where the postings in question were not libelous). Plaintiff here is able to demonstrate each one of these factors.

First, Plaintiff has sufficiently identified the Doe Defendants through the unique IP address each Doe Defendant was assigned at the time of the unauthorized distribution of the copyrighted Work. *See* Hansmeier Decl. ¶ 16; *Seescandy.com*, 185 F.R.D. at 578–80. These Defendants gained access to the Internet through their respective ISPs (under cover of an IP address) only by setting up an account with the various ISPs. (*See generally* Hansmeier Decl.) The ISPs can identify each Defendant by name through the IP address by reviewing its subscriber activity logs. (*See id.* ¶¶ 21–22.) Thus, Plaintiff can show that all Defendants are “real persons” whose names are known to the ISP and who can be sued in federal court.

Second, Plaintiff has specifically identified the steps taken to identify Defendants' true identities. (*See* Hansmeier Decl. ¶¶ 21–23.) Plaintiff has obtained each Defendant's IP address and the date and time of the Defendant's infringing activities, has traced each IP address to specific ISPs, and has made copies of the Work each Defendant unlawfully distributed or made

available for distribution. (*See id.* ¶ 19.) Therefore, Plaintiff has obtained all the information it possibly can about the Defendants without discovery from the ISPs.

Third, Plaintiff has asserted a prima facie claim for direct copyright infringement in its Complaint that can withstand a motion to dismiss. Specifically, Plaintiff has alleged that: (a) it owns the exclusive licensing and distribution rights, and the exclusive rights under the registered copyright for the Work, and (b) the Doe Defendants copied or distributed the copyrighted Work without Plaintiff's authorization. (*See generally* Compl.) These allegations state a claim for copyright infringement. See 17 U.S.C. § 106(1)(3); *In re Aimster Copyright Litig.*, 334 F.3d 643, 645 (7th Cir. 2003), *cert. denied*, 124 S. Ct. 1069 (2004) (“Teenagers and young adults who have access to the Internet like to swap computer files containing popular music. If the music is copyrighted, such swapping, which involves making and transmitting a digital copy of the music, infringes copyright.”); *A & M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1014–15 (9th Cir. 2001) (“Napster users who upload file names to the search index for others to copy violate plaintiffs’ distribution rights. Napster users who download files containing copyrighted music violate plaintiffs’ reproduction rights.”). Courts have wide discretion in discovery matters and have also allowed expedited discovery when “good cause” is shown. *See Warner Bros. Records, Inc. v. Does 1–6*, 527 F. Supp. 2d 1, 2 (D.D.C. 2007); *Qwest Comm. Int’l, Inc. v. WorldQuest Networks, Inc.*, 213 F.R.D. 418, 419 (D. Colo. 2003); *Entm’t Tech. Corp. v. Walt Disney Imagineering*, No. Civ. A. 03-3546, 2003 WL 22519440, at *4 (E.D. Pa. 2003) (applying a reasonableness standard and finding that “a district court should decide a motion for expedited discovery on the entirety of the record to date and the reasonableness of the request in light of all of the surrounding circumstances.”) (internal quotations omitted); *Semitoil, Inc. v. Tokyo*

Electron Am., Inc., 208 F.R.D. 273, 275–76 (N.D. Cal. 2002); *Yokohama Tire Corp. v. Dealers Tire Supply, Inc.*, 202 F.R.D. 612, 613–14 (D. Ariz. 2001) (applying a good cause standard).

Good cause exists here because ISPs typically retain user activity logs containing the information sought for only a limited period of time before erasing the data. (*See* Hansmeier Decl. ¶ 22.) If that information is erased, Plaintiff will have no ability to identify the Defendants, and thus will be unable to pursue its lawsuit to protect its copyrighted work. (*Id.*) Where “physical evidence may be consumed or destroyed with the passage of time, thereby disadvantaging one or more parties to the litigation,” good cause for discovery before the Rule 26 conference exists. *Qwest Comm.*, 213 F.R.D. at 419; *see also Pod-Ners, LLC v. N. Feed & Bean of Lucerne LLC*, 204 F.R.D. 675, 676 (D. Colo. 2002) (allowing discovery prior to Rule 26 conference to inspect items in defendant’s possession because items might no longer be available for inspection if discovery proceeded in the normal course).

Good cause exists here for the additional reason that a claim for copyright infringement presumes irreparable harm to the copyright owner. *UMG Recordings, Inc. v. Doe*, 2008 WL 4104214 (N.D. Cal. 2008) (finding that good cause for expedited discovery exists in Internet infringement cases, where a plaintiff makes a prima facie showing of infringement, there is no other way to identify the Doe defendant, and there is a risk an ISP will destroy its logs prior to the conference); *see also Elvis Presley Enter., Inc. v. Passport Video*, 349 F.3d 622, 631 (9th Cir. 2003); I4 Melville B. Nimmer & David Nimmer, *Nimmer on Copyright*, § 14.06[A], at 14-03 (2003). The first and necessary step that Plaintiff must take to stop the infringement of its valuable copyright is to identify the Doe Defendants who are copying and distributing the Work. This lawsuit cannot proceed without the limited discovery Plaintiff seeks because the ISPs are the only entities that can identify the otherwise anonymous Defendants. Courts regularly permit

early discovery where such discovery will “substantially contribute to moving th[e] case forward.” *Semitoool*, 208 F.R.D. at 277.

Finally, Defendants have no legitimate expectation of privacy in the subscriber information they provided to the ISPs, much less in downloading and distributing the copyrighted Work without permission. *See Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) (“[C]omputer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person—the system operator.”); *Interscope Records v. Does 1–14*, 558 F. Supp. 2d 1176, 1178 (D. Kan. 2008) (a person using the Internet to distribute or download copyrighted music without authorization is not entitled to have their identity protected from disclosure under the First Amendment); *Arista Records, LLC v. Doe No. 1*, 254 F.R.D. 480, 481 (E.D.N.C. 2008); *Sony Music Entm’t, Inc. v. Does 1–40*, 326 F. Supp. 2d 556, 566 (S.D.N.Y. 2004) (“[D]efendants have little expectation of privacy in downloading and distributing copyrighted songs without permission.”); *United States v. Hambrick*, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999), *aff’d*, 225 F.3d 656 (4th Cir. 2000). This is because a person can have no legitimate expectation of privacy in information he or she voluntarily communicates to third parties. *See, e.g., Smith v. Maryland*, 442 U.S. 735, 743–44 (1979); *United States v. Miller*, 425 U.S. 435, 442–43 (1976); *Couch v. United States*, 409 U.S. 322, 335–36 (1973); *Guest v. Leis*, 255 F.3d at 335; *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000); *Hambrick*, 55 F. Supp. 2d at 508.

Although Defendants copied and distributed the Work without authorization using fictitious user names, their conduct was not thus anonymous. Using publicly available technology, the unique IP address assigned to each Defendant at the time of infringement can be readily identified. (*See Hansmeier Decl.* ¶ 15.) When Defendants entered into a service

agreement with the ISPs, they knowingly and voluntarily disclosed personal identification information to it. As set forth above, this identification information is linked to the Defendants' IP address at the time of infringement, and recorded in the ISPs' respective subscriber activity logs. Since Defendants can, as a consequence, have no legitimate expectation of privacy in this information, this Court should grant Plaintiff leave to seek expedited discovery of it. Absent such leave, Plaintiff will be unable to protect its copyrighted Work from continued infringement.

Where federal privacy statutes authorize disclosure pursuant to a court order, courts have held that a plaintiff must make no more than a showing of relevance under the traditional standards of Rule 26. *See Laxalt v. McClatchy*, 809 F.2d 885, 888 (D.C. Cir. 1987) (finding "no basis for inferring that the statute replaces the usual discovery standards of the FRCP . . . with a different and higher standard"); *Pleasants v. Allbaugh*, 208 F.R.D. 7, 12 (D.D.C. 2002); *accord Lynn v. Radford*, No. 99-71007, 2001 WL 514360, at *3 (E.D. Mich. Mar. 16, 2001); *Gary v. United States*, No. 3:97-CV-658, 1998 WL 834853, at *4 (E.D. Tenn. Sept. 4, 1998); *see also In re Gren*, 633 F.2d 825, 828 n.3 (9th Cir. 1980) (finding that the "court order" provision of Fair Credit Reporting Act requires only "good faith showing that the consumer records sought are relevant") (internal quotation omitted). Plaintiff clearly has met that standard, as the identity of Defendants is essential to Plaintiff's continued prosecution of this action.

III. CONCLUSION

For the foregoing reasons, Plaintiff respectfully submits that the Court should grant the Motion for Leave to Take Discovery Prior to Rule 26 Conference and enter an Order substantially in the form of the attached Proposed Order.

Respectfully submitted,

AF Holdings LLC

DATED: January 13, 2012

By: /s/ Paul A. Duffy
Paul A. Duffy, Esq. (D.C. Bar Number: IL0014)
Prenda Law Inc.
161 N. Clark St., Suite 3200
Chicago, IL 60601
Telephone: (312) 880-9160
Facsimile: (312) 893-5677
E-mail: paduffy@wefightpiracy.com
Counsel for the Plaintiff

LOCAL CIV. R. 7(m) CERTIFICATION

Because Plaintiff does not currently know the identity of any of the Defendants, Plaintiff cannot ascertain the position of any of the Defendants on this Motion.

DATED: January 13, 2012

By: /s/ Paul A. Duffy
Paul A. Duffy, Esq.